CISA ALERT (AA21-131A)

DARKSIDE RANSOMWARE: BEST PRACTICES FOR PREVENTING BUSINESS DISRUPTION FROM RANSOMWARE ATTACKS

In the wake of the Colonial Pipeline cyberattack, the FBI and CISA released a cybersecurity advisory for public consumption on preventing and mitigating ransomware attacks. While this does reference the Colonial Pipeline cyberattack, and is slanted toward the critical infrastructure industry, this information is relevant to almost all businesses.

https://us-cert.cisa.gov/ncas/alerts/aa21-131a

On this webpage, the CISA also provides links to multiple resources for the prevention and mitigation of ransomware, general cybersecurity, and detecting, responding to, and recovering from attacks. These links are applicable to many industries.

CISA - Cyber Hygiene Services

As a reminder, the CISA may be able to provide several free cyber hygiene services to federal, state, local, tribal and territorial governments, as well as public and private sector critical infrastructure organizations.

Services may include:

- Vulnerability Scanning
- Web Application Scanning
- Phishing Campaign Assessment
- Remote Penetration Test

These free services may be critical for many organizations in preventing and mitigating these types of cyberattacks. For more information about these services, please visit the CISA webpage at:

https://www.cisa.gov/cyber-hygiene-services

Glatfelter℠ PUBLIC ENTITIES